Information Technology

PAT McCRORY
Governor

KEITH WERNER
State Chief Information Officer

June 27, 2016

MEMORANDUM

TO: State CIOs and State Security Liaisons

FROM: Maria S. Thompson
State Chief Risk Officer

SUBJECT: Implementation Guidance for Annual Legislative Reporting of Security Assessment and Compliance – Continuous Monitoring Plan

A. OVERVIEW:

The State Chief Information Officer (SCIO), is charged with ensuring that the State agencies and State data are operating in compliance with the set enterprise security standards. In order to accomplish this task, the Enterprise Security and Risk management Office (ESRMO) has developed a Continuous Monitoring Plan to address the management of risk assessments and compliance reporting throughout the State. Risk assessments are a sub-component of the Continuous Monitoring Plan and ensures the assessments, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information it processes, stores, or transmits, is mitigated to the highest level of fidelity. The Continuous Monitoring Plan leverages industry best practices using the National Institute of Standards and Technology (NIST) Special Publication 800-37 – Continuous Monitoring Process as a guideline (see figure 1).

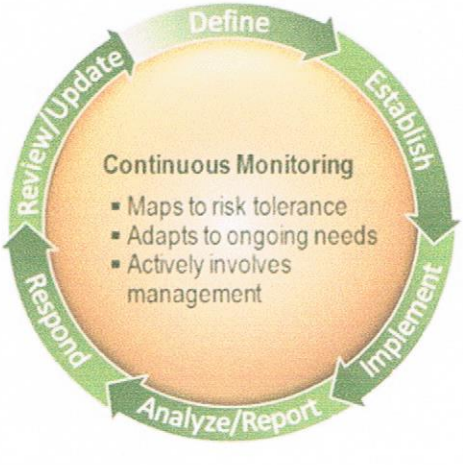

Figure 1 – NIST Special Publication 800-137 Continuous Monitoring Process

B. BACKGROUND:

Pursuant to N.C.G.S. 143B-1376 the State CIO must annually assess the ability of each agency and each agency's contracted vendors to comply with the current enterprise-wide set of security standards. The information gathered from each assessment will be used to build out the State IT Plan. These assessments will include, at a minimum:

1. Rate of compliance with the enterprise-wide security standards
2. Estimate of cost to implement deficient security measures
3. Assessment of Security Organization
    a) Security practices
    b) Security industry standards
    c) Network security architecture
    d) Current expenditures of State funds for Information Technology (IT) security

In addition, the State CIO is to annually certify by October 1, that State data held in **non-State facilities** is being maintained in accordance with State IT security standards. This certification will be provided annually to the Joint Legislative Oversight Committee on IT and Fiscal Research Division.

C. CONTINUOUS MONITORING (CM) PLAN:

In order to meet the intent of N.C.G.S. 143B-1376, ESRMO has developed a Continuous Monitoring Plan which requires that all agencies complete an annual risk and security assessment of their critical systems and infrastructure and that there are ongoing processes in place to assess the current posture of the environment. The Continuous Monitoring Plan is designed as a three-year program to ensure that all agencies are assessed using one or a combination of assessment methods identified below:

- Third Party Independent Assessment (Vendor or National Guard)
- Self-Assessment

All Agencies **MUST** complete an assessment annually. It is the agency's responsibility to ensure that an appropriate budget amount is requested to meet the needs of the legislative mandate. The Department of Information Technology (DIT), ESRMO may conduct compliance readiness reviews within the Executive Branch agencies to validate cyber readiness.

Within 30 days of completion of an assessment, all agencies are required to provide ESRMO with the results and a plan to remediate the findings. During this calendar year, ESRMO will be deploying an Enterprise Governance, Risk and Compliance (EGRC) tool to automate this process. This tool will be used to create and maintain corrective actions plans for those deficiencies noted during a risk assessment, including vulnerability scans, and will ensure:

- Accurate reporting on the status of corrective actions;
- Development of a process to evaluate supporting documentation and the time to monitor recommendations;
- Coordination between the agencies and ESRMO in order to address residual risks for those controls that cannot be implemented.

For this initial reporting period, agencies are required to use the Corrective Action Plan spreadsheet located at https://it.nc.gov/document/corrective-action-plan-cap-and-instructions

D. CONTRACTED VENDORS (CLOUD SERVICE PROVIDERS (CSP)):

Assessment of agency compliance with security standards, requires agencies who have contracted with cloud-hosted solutions or off-site hosting services, to obtain prior approval from the State CIO, and also ensure vendor compliance with Statewide security policies. Agencies will ensure that contract language requires vendors to provide as attestation to their compliance, an industry recognized, third party assessment report. Procurement language must also require, in addition to initial validation, cloud/vendor must annually provide the agency validation of their continued compliance to State policies and procedures. This requirement includes all vendors supporting Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and/or Software as a Service (SaaS). Examples of acceptable assessment reports include, Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, SSAE 16 and ISO 27001. CSPs must demonstrate to the State that ongoing continuous monitoring activities are in place and compliance is being met for the following requirements:

- Security
- Privacy
- Confidentiality
- Availability (Business Continuity Management)
- Processing Integrity

Agencies are required to review these report, assess the risk of each vendor and provide annual certification to their compliance to the State CIO. N.C.G.S. 143B-1376.

E. DATA INVENTORY

Statewide security standards, N.C.G.S. § 143B-1376 requires that all agencies maintain a data inventory of all cloud hosted services in use within their agencies. In order to accomplish this, each agency must complete a Privacy Threshold Analysis (PTA) document detailing the data classification and data fields being hosted within a cloud, offsite or vendor hosted environment. The PTA must be reviewed at minimum annually, and when changes are made to the data being collected through interconnections with systems of differing levels of sensitivity or other collection methods.

F. REQUIREMENT:

1. Assessments

Beginning in Calendar year 2016, each Agency must conduct either an agency-wide third party assessment of all critical systems and associated security controls or complete an ESRMO provided self-assessment questionnaire. As mentioned in paragraph C, third party assessments will be conducted on a 3-year cycle. Agencies that completed an agency-wide third party assessment in year 1, may opt to complete a self-assessment or a more targeted and system specific assessment during years 2-3. All critical systems hosting data classified as Restricted or Highly Restricted, in compliance with the Statewide Data Classification and Handling Policy **MUST** receive an independent third party assessment at minimum every 3 years or as mandated by governing Federal entity.

For CY 2016, the self-assessment will be conducted using the Department of Homeland Security, Cybersecurity Evaluation Tool (CSET). CSET uses the NIST Cybersecurity Framework and provides agencies "a systematic and repeatable approach for assessing the security posture of their cyber systems and networks." This tool will facilitate the consolidation of agency reports and provide a summary of compliance with industry best practices and state requirements. Note: CSET cannot reveal all types of security weaknesses, and should **not** be the sole means of determining an agency's security posture. It is recommended that the assessment be completed using a cross functional team consisting of representatives from operational, maintenance, information technology, business, and security. The representatives must be subject matter experts with significant expertise in their respective areas. The CSET application and self-assessment instructions are available for download from the ESRMO external SharePoint site. https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/CSET%207.0

2. Security/Budget Deficiencies

Annual reports must ensure that the agency has identified their security deficiencies and estimated cost for remediation. The report may include, but is not limited to the following items:

- Security boundary devices, e.g. firewalls, intrusion detection/prevention systems (IDPS)
- Vulnerability management e.g. scanning and patching systems
- Personnel shortfalls
- Cybersecurity training deficiencies
- End-of-life systems

All State agencies are required to provide the State CIO their annual compliance and assessments reports, annually **no later than** September 1 of the given Calendar Year (CY). This certification includes compliance of cloud service providers. Agencies will use the templates provided in Appendix A for their reporting. Any deficiencies identified within the agency which would preclude them from being compliant, must be addressed using the Corrective Action Plan (CAP) template. Instructions and the template can be downloaded from the site noted above. This document will be submitted along with Appendix A in order to sufficiently address this requirement. Reports must be submitted using approved encryption methods.

The point of contact (POC) for this correspondence is the State Chief Risk Officer, Maria Thompson, maria.s.thompson@nc.gov (919) 754-6578.

APPENDIX A – AGENCY ANNUAL ASSESSMENT AND COMPLIANCE REPORT TEMPLATE

TO:	Keith Werner State Chief Information Officer
FROM:	[AGENCY]
SUBJECT:	[ENTER Calendar Year XXXX] Agency Compliance Report

Pursuant to the authorities and powers of the State Chief Information Officer enumerated in Session Law 2015-241, and as Agency head for [AGENCY];

□ I certify that [AGENCY] has implemented the appropriate processes and procedures to be in compliance with the Statewide Information Security Manual, G.S. § 143B-1341, 143B-1342 and § 143B-1343 to include:

- No data of a confidential nature, as defined in the General Statutes or federal law, was entered into or processed through any information technology system or network established under this Article until safeguards for the data's security satisfactory to the State CIO have been designed and installed and are fully operational.

- Obtaining approval from the State CIO prior to contracting for the storage, maintenance, or use of State data by a private vendor.

- Ensuring all information technology security goods, software, or services purchased using State funds, or for use by a State agency or in a State facility, was subject to approval by the State CIO in accordance with security standards

- Completion of annual risk assessments to identify compliance, operational, and strategic risks to the enterprise network. These assessments may include methods such as penetration testing or similar assessment methodologies.

- All contracts for third party assessment and testing, was approved by the State CIO. Resulting sanitized assessment reports were made public.

- Incident Reporting Compliance– Providing the full details of the State agency's information technology and operational requirements and of all the agency's information technology security incidents within 24 hours of confirmation

- Designating an agency liaison in the information technology area to coordinate with the State CIO.

- Completed annual assessment of the agency's contracted vendors, to comply with the current security enterprise-wide set of standards. The assessment shall include, at a minimum, the rate of compliance with the enterprise-wide security standards and an assessment of security organization, security practices, security information standards, network security architecture, and current expenditures of State funds for information technology security.
- Submit disaster recovery plans to the State CIO on an annual basis and as otherwise requested by the State CIO

□ [AGENCY] has not completed all requirements but have identified a plan to be in compliance. Attached is our assessment report to include corrective action plan indicating when the agency will meet these requirements.

In accordance with § 143B-1342, below is the estimated cost to implement security measures needed for agencies to fully comply with the standards.

SECURITY / BUDGET DEFICIENCIES:

1. **Security Boundary Devices**:

[INSERT JUSTIFICATION/COMMENTS]

Cost to Remediate: ________________________

2. **Personnel**:

[INSERT JUSTIFICATION/COMMENTS]

Cost to Remediate: ________________________

3. **Cybersecurity Training:**

[INSERT JUSTIFICATION/COMMENTS]

Cost to Remediate: ________________________

4. **Vulnerability Management:**

[INSERT JUSTIFICATION/COMMENTS]

Cost to Remediate: ________________________

5. **End of Lifecycle Systems:**

[INSERT JUSTIFICATION/COMMENTS]

Cost to Remediate: ______________________

For additional information about this submission please contact: [INSERT AGENCY CONTACT]

____ ____

Printed Name of Secretary/Director or Designee [Signature] [Date]